DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Po-We Chen, Reg. No. 61,767 on 01 September 2010.

1. Replace claims 8, 11 and 12 with the following (shown ***marked up*** here, followed by *clean version*):

8. A quantum-key distributing method for a quantum cryptographic system including a transmission-side communication apparatus that transmits a random number sequence forming a basis of an encryption key in a predetermined quantum state on a quantum communication path and a reception-side communication apparatus that measures a photon on the quantum communication path, the quantum-key distributing method comprising: transmitting and receiving including the reception-side communication apparatus maintaining reception data with probability information obtained as a result of measuring a light direction with a measuring device for correctly identifying the light direction; and the transmission-side communication apparatus maintaining transmission data corresponding to the reception data; information

notifying including the transmission-side communication apparatus notifying, via a public communication path, the reception-side communication apparatus of error correction information generated based on a parity check matrix, of which elements are "0" or "1", and the transmission data and error detection information generated based on a cyclic code for detecting an error and the transmission data; transmission-data estimating including the reception-side communication apparatus estimating the transmission data based on a same parity check matrix as that of the transmission-side communication apparatus, the reception data with probability information, the error correction information, and the error detection information; and encryption-key generating including the transmission-side communication apparatus and the reception-side communication apparatus discarding a part of the transmission data according to an amount of ~~open information~~ information laid open to the public communications path and generating an encryption key using rest of the transmission data.

11. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and transmits a random number sequence forming a basis of the encryption key to a quantum communication path in a predetermined quantum state, the communication apparatus comprising: an information notifying unit that notifies, via a public communication path, the other apparatus of error correction information and error detection information, the error correction information being generated based on transmission data corresponding to reception data of the other apparatus obtained as a result of measuring a light direction with a measuring device for correctly identifying the light direction and a same parity check matrix as that of the other apparatus, the error detection

information being generated based on the transmission data and a cyclic code for detecting an error; and an encryption-key generating unit that discards a part of the transmission data according to an amount of ~~open information~~ information laid open to the public communications path, and generates an encryption key using rest of the transmission data.

12. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and measures a photons, which is a random number sequence forming a basis of the encryption key, on a quantum communication path, the communication apparatus comprising: a transmission-data estimating unit that estimates original transmission data based on a parity check matrix identical to that of other apparatus that shares the encryption key, reception data with probability information obtained by measuring a light direction with a measuring device for correctly identifying the light direction, and error correction information and error detection information received from other apparatus via a public communication path; and an encryption-key generating unit that discards a part of the transmission data according to an amount of ~~open information~~ information laid open to the public communications path, and generates an encryption key using rest of the transmission data.

clean version:

8. A quantum-key distributing method for a quantum cryptographic system including a transmission-side communication apparatus that transmits a random number sequence forming a

basis of an encryption key in a predetermined quantum state on a quantum communication path and a reception-side communication apparatus that measures a photon on the quantum communication path, the quantum-key distributing method comprising: transmitting and receiving including the reception-side communication apparatus maintaining reception data with probability information obtained as a result of measuring a light direction with a measuring device for correctly identifying the light direction; and the transmission-side communication apparatus maintaining transmission data corresponding to the reception data; information notifying including the transmission-side communication apparatus notifying, via a public communication path, the reception-side communication apparatus of error correction information generated based on a parity check matrix, of which elements are "0" or "1", and the transmission data and error detection information generated based on a cyclic code for detecting an error and the transmission data; transmission-data estimating including the reception-side communication apparatus estimating the transmission data based on a same parity check matrix as that of the transmission-side communication apparatus, the reception data with probability information, the error correction information, and the error detection information; and encryption-key generating including the transmission-side communication apparatus and the reception-side communication apparatus discarding a part of the transmission data according to an amount of information laid open to the public communications path and generating an encryption key using rest of the transmission data.

11. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and transmits a random

number sequence forming a basis of the encryption key to a quantum communication path in a predetermined quantum state, the communication apparatus comprising: an information notifying unit that notifies, via a public communication path, the other apparatus of error correction information and error detection information, the error correction information being generated based on transmission data corresponding to reception data of the other apparatus obtained as a result of measuring a light direction with a measuring device for correctly identifying the light direction and a same parity check matrix as that of the other apparatus, the error detection information being generated based on the transmission data and a cyclic code for detecting an error; and an encryption-key generating unit that discards a part of the transmission data according to an amount of information laid open to the public communications path, and generates an encryption key using rest of the transmission data.

12. A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and measures a photons, which is a random number sequence forming a basis of the encryption key, on a quantum communication path, the communication apparatus comprising: a transmission-data estimating unit that estimates original transmission data based on a parity check matrix identical to that of other apparatus that shares the encryption key, reception data with probability information obtained by measuring a light direction with a measuring device for correctly identifying the light direction, and error correction information and error detection information received from other apparatus via a public communication path; and an encryption-key generating unit that

discards a part of the transmission data according to an amount of information laid open to the public communications path, and generates an encryption key using rest of the transmission data.

Examiner's Statement of Reasons for Allowance

2. Claims 8-14 are allowed over prior art.

3. This action is in reply to applicant's correspondence of 29 June 2010.

4. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

5. As per claims 8, 11 and 12 generally, prior art of record Buttler, W., et al, ' Fast, efficient error reconciliation for quantum cryptography ', Univ. of Ca., Los Alamos National Laboratory, Los Alamos, NM 87545, (March 20, 2002), entire document, http://cdsweb.cern.ch/record/543746/files/0203096.pdf ("Buttler"), fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 29 June 2010 to office action of 21 April 2010.

Specifically, (as per claim 8, for example) prior art dealing with QKD aspects of key information communications between the source and destination cryptographic apparatus, insofar as quantum probability information associated with the key (irrespective of the key content per se) communicated across the source/destination communications path (i.e., QKD based shared key distribution, insofar as reconciliation of Gaussian key elements via extracting common information out of any shared variables (as applied to the special case of Gaussian key elements), so as to generate/distribute the key as a function of the shared extracted Gaussian key elements – irrespective of leakage of information, and the details of how the information involved in

generating the key is transferred between the source and destination; Assche, G.V., et al, ' Reconciliation of a Quantum-Distributed Gaussian Key ', IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 50, NO. 2, FEBRUARY 2004, pp. 394-400, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.2483&rep=rep1&type=pdf) is known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., ***error detection/correction probability*** information for the *measured light direction* of the key information in the form of ***a parity check matrix***, and transferred ***via a public communication path*** in support of the key generation/distribution, insofar as using the ***error detection/correction probability*** information for ***discarding a part of the transmission data*** as a function of ***an amount of information laid open to the public communications path*** in the key generation per se), ***at the time*** *of the invention*; serving to patently distinguish the invention from said prior art;

"8. A *quantum-key distributing method* for a quantum cryptographic system including a transmission-side communication apparatus that *transmits a random number sequence forming a basis of an encryption key* in a predetermined quantum state on a quantum communication path and a reception-side communication apparatus that measures a photon on the quantum communication path, the quantum-key distributing method comprising:

transmitting and receiving including

the *reception-side communication apparatus* ***maintaining***

reception data with probability information *obtained as a result of measuring a light direction with a measuring device for correctly identifying the light direction*; and

the transmission-side communication apparatus maintaining

transmission data corresponding to

the reception data;

information notifying including

*the **transmission-side** communication apparatus **notifying,***

***via a public communication path**,*

the ***reception-side** communication apparatus **of***

***error correction** information generated*

***based on a parity check matrix**,*

of which elements are "0" or "1", and

the transmission data and error detection information

generated based on

a cyclic code for detecting an error and

the transmission data;

*transmission-data **estimating including***

the *reception-side* communication apparatus

***estimating the transmission data** based on*

a ***same parity check matrix*** as that of

the transmission-side communication apparatus,

the ***reception** data **with probability** information*,

the ***error correction** information*, and

the ***error detection** information*; and

*encryption-key **generating*** including

the ***transmission-side*** communication apparatus and

the ***reception-side*** communication apparatus

discarding a part of the transmission data according to

an amount of information

laid open to the public communications path and

generating an encryption key

using rest of the transmission data.".

6. Dependent claims 9, 10, 13 and 14 are allowable by virtue of their dependencies.

Conclusion

7. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad, can be reached at (571) 272-7884. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439